Department of Homeland Security

Information Analysis and Infrastructure Protection
Advisory 03-_____

April 10, 2003

"Remote Sendmail Vulnerability"

ATTN: *Network Security Officers*

SUMMARY:

The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) is issuing this advisory to heighten awareness of a remotely exploitable vulnerability in Sendmail. DHS / IAIP is working closely with the information technology industry to improve vulnerability awareness and information dissemination.

DHS / IAIP received confirmation that this vulnerability, initially discovered by Michal Zalewski, was exploited in a laboratory environment. Industry representatives have also verified that an exploit for this vulnerability exists in the wild. The probability of continued exploitation is high.

This vulnerability in Sendmail may be exploited to cause a denial-of-service state, or may allow local and/or remote intruders the ability to gain super-user (root) access/control of a vulnerable Sendmail server. This vulnerability can be exploited through a simple e-mail message containing malicious code. Because address parsing code in vulnerable versions Sendmail does not check the length of email addresses sufficiently, a successful attacker could install malicious code, run destructive programs and modify or delete files by simply sending a specially crafted malicious email to or through a vulnerable server. Many Sendmail servers are not shielded by perimeter defense mechanisms since they typically do not inspect email headers for malicious code, only the body or attachments.

Additionally, attackers may gain access to other systems thru a compromised Sendmail server, depending on local configurations. Sendmail versions 5.2 up to 8.12.8 are known to be vulnerable at this time. Sendmail versions 8.12.9 and 8.11.7 provide some (not complete) protection for other vulnerable Sendmail servers. System administrators are urged not to rely solely on this limited protection and to take appropriate measures.

DESCRIPTION:

The Remote Sendmail Vulnerability is initiated by the contents of specially crafted email messages. Mail-Transfer-Agents (MTA) that do not contain the vulnerability will pass the malicious message along to other MTAs that may be protected at the network level. Messages capable of exploiting this vulnerability may pass undetected through many common packet filters or firewalls. The vulnerability allows a remote attacker to gain access to the Sendmail server by sending an e-mail containing a specially crafted address field that triggers a buffer overflow.

RECOMMENDATION:

Due to the seriousness of this vulnerability and the recent exploits of Sendmail, DHS / IAIP encourages administrators to take this opportunity to review the security of their Sendmail systems implementations as soon as possible. DHS / IAIP strongly recommends that system administrators who employ Sendmail and who have not already taken corrective action do so now.

Patches and additional information regarding the vulnerability are available from Sendmail, ISS, CERT-CC, and from vendors whose applications incorporate Sendmail code, including IBM, HP, SUN, and Red Hat Inc. Other vendors have released patches or are investigating the release of patches in the near future.

Vendor information can be obtained from:
http://www2.fedcirc.gov/advisories/ FA-2003-12.html
http://www.kb.cert.org/vuls/id/897604

The primary distribution site for Sendmail is:

http://www.sendmail.com/security/
ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu
ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu.asc.

The Internet Security Systems, Inc. Download center
http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=22127

Additional information may be obtain from:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0161

As always, computer users are advised to keep their anti-virus, other security software and systems software current by checking their vendor's web sites frequently for new updates and to check for alerts put out by the DHS / IAIP, CERT/CC, ISS and other cognizant organizations.

DHS encourages individuals to report information concerning suspicious or criminal activity to law enforcement or a Homeland Security watch office. Individuals may report incidents online at http://www.nipc.gov/incident/cirr.htm, and Federal agencies/departments may report incidents online at http://www.fedcirc.gov/reportform.html. Contact numbers for the IAIP watch centers are: (202) 323-3205, 1-888-585-9078, or nipc.watch@fbi.gov; for the telecom industry, (703) 607-4950 or ncs@ncs.gov; and for Federal agencies/departments, (888) 282-0870 or fedcirc@fedcirc.gov.

IAIP intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory Level is anticipated; the current level is Orange.